

**CIPHER COMMUNICATION METHOD AND STORAGE MEDIUM  
RECORDING ITS PROGRAM**

**Publication number:** JP2000278260 (A)

**Publication date:** 2000-10-06

**Inventor(s):** ITO MASARU

**Applicant(s):** HITACHI INFORMATION SYS LTD

**Classification:**

- international: **G06F13/00; H04L9/14; H04L29/08; G06F13/00; H04L9/14; H04L29/08; (IPC1-7): H04L9/14; G06F13/00; H04L29/08**

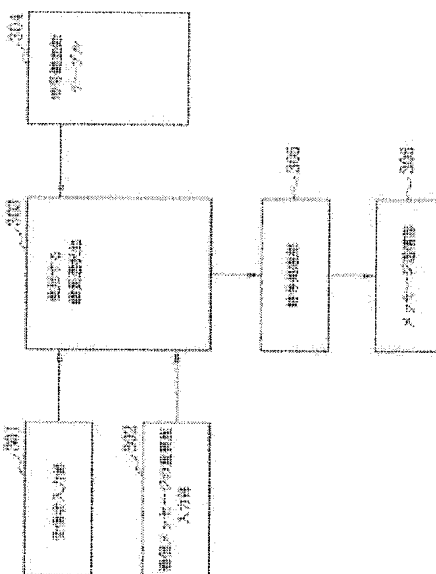
- European:

**Application number:** JP19990079871 19990324

**Priority number(s):** JP19990079871 19990324

**Abstract of JP 2000278260 (A)**

**PROBLEM TO BE SOLVED:** To relieve the load of a sender and to save computer resources by allowing a user of cipher communication to select an optimum encryption algorithm while keeping the security of the cipher communication under a network computing environment. **SOLUTION:** A key length selection section 303 retrieves an encryption algorithm and an encryption key from an encryption key registration table 304 by using a recipient ID entered to a recipient entry section 301 and converted into a network class and importance information entered to a communication message importance entry section 302 as keys, and an encryption processing section 305 encrypts a message by using them when the result of retrieval shows the encryption algorithm and encryption key are existent and a message transmission section 306 transmits the encrypted message via a communication channel. When the result of retrieval shows they are not existent in the table, the message is transmitted as a plain message without being encrypted.



Data supplied from the **esp@cenet** database — Worldwide

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-278260

(P2000-278260A)

(43) 公開日 平成12年10月6日(2000.10.6)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード*(参考)	
H 0 4 L 9/14	3 5 1	H 0 4 L 9/00	6 4 1	5 B 0 8 9
G 0 6 F 13/00		G 0 6 F 13/00	3 5 1 Z	5 J 1 0 4
H 0 4 L 29/08		H 0 4 L 13/00	3 0 7 Z	5 K 0 3 4

審査請求 未請求 請求項の数 4 O L (全 7 頁)

(21) 出願番号 特願平11-79871

(22) 出願日 平成11年3月24日(1999.3.24)

(71) 出願人 000152985

株式会社日立情報システムズ

東京都渋谷区道玄坂1丁目16番5号

(72) 発明者 伊藤 優

東京都渋谷区道玄坂一丁目16番5号 株式会社日立情報システムズ内

(74) 代理人 100077274

弁理士 磯村 雅俊 (外1名)

Fターム(参考) 5B089 GA21 GB04 HA10 JA03 JA08

JA31 JB22 KA05 KA06 KB06

KB13 KC53 KH30

5J104 AA01 AA35 NA02 NA37 PA07

5K034 AA05 AA07 AA10 BB06 CC01

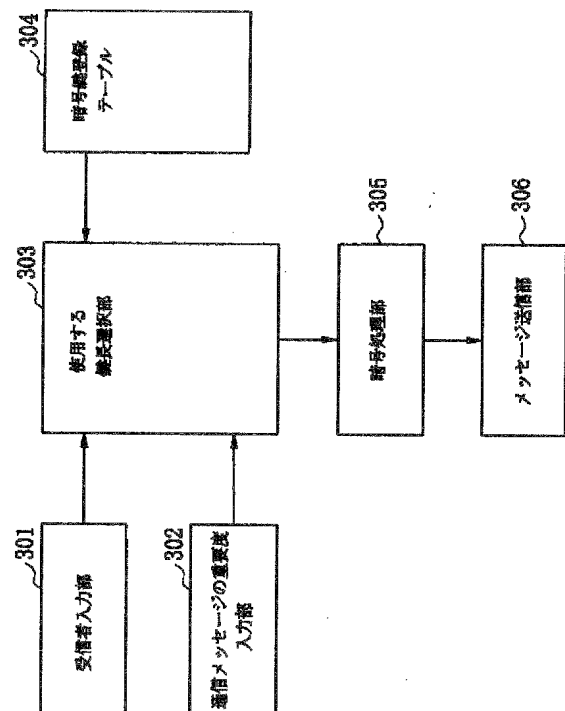
HH01 HH14 HH16 HH63

(54) 【発明の名称】 暗号通信方法およびそのプログラムを記録した記録媒体

(57) 【要約】

【課題】 ネットワークコンピューティング環境下で、暗号通信の利用者は暗号通信の安全性を確保しながら、最適な暗号アルゴリズムを選択し、送信者の負担を軽減しコンピュータ資源の節約を図る。

【解決手段】 受信者入力部301に入力された受信者IDをネットワーク種別に変換し、かつ通信メッセージの重要度入力部302に入力された重要度とをキーとして、鍵長選択部303は暗号鍵登録テーブル304から暗号アルゴリズムと暗号鍵を検索し、検索の結果が有れば、暗号処理部305でそれらを用いて暗号化し、メッセージ送信部306から通信回線を介して暗号メッセージ送信する。検索の結果、テーブルに該当するものがなければ、暗号化せずに平文で送信する。



## 【特許請求の範囲】

【請求項 1】 コンピュータネットワーク上で暗号メッセージ通信を行うメッセージ通信方法において、暗号通信メッセージの受信者名が入力されると、該受信者名に基づき使用されるネットワークの種別を算出し、通信メッセージの秘匿の必要性の段階が入力されると、該ネットワークの種別およびメッセージの秘匿の必要性の段階をキーとして、暗号鍵登録テーブル中から使用すべき暗号アルゴリズムと暗号鍵を検索し、検索の結果、該当する暗号アルゴリズムと暗号鍵が存在すれば、該暗号アルゴリズムと暗号鍵でメッセージを暗号化し、暗号されたメッセージを送信することを特徴とする暗号通信方法。

【請求項 2】 前記暗号鍵登録テーブルには、ネットワークの種別とメッセージ重要度に対応して、暗号アルゴリズムと暗号鍵が登録されていることを特徴とする請求項 1 に記載の暗号通信方法。

【請求項 3】 前記暗号通信メッセージの受信者名が入力されると、受信者名と IP アドレスとがマッピングされたデータベースにより、該当する IP アドレスが抽出され、該当 IP アドレスより使用される通信回線が判別されることを特徴とする請求項 1 に記載の暗号通信方法。

【請求項 4】 請求項 1～3 のうちのいずれかに記載の暗号通信方法の処理をプログラムに変換し、変換されたプログラムを記録したことを特徴とする記録媒体。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】 本発明は、ネットワークコンピュータ環境で、暗号メッセージ通信を行うメッセージ通信方法およびそのプログラムを記録した記録媒体に関し、特に種々のネットワークを使用し、かつ通信メッセージの重要性に応じて必要な暗号アルゴリズムと必要な長さの暗号鍵を選択して送信することができるので、必要な強度の暗号文が得られるとともに、暗号化に伴う費用を低減することができる暗号通信方法およびそのプログラムを記録した記録媒体に関する。

## 【0002】

【従来の技術】 ネットワークコンピュータ環境下で暗号メッセージ通信を行う場合、秘密鍵暗号（慣用暗号）を用いる第 1 の方法と公開鍵暗号を用いる第 2 の方法がある。秘密鍵暗号を使用する場合には、送信者と受信者が予め定められた同一の暗号鍵を保有しておき、送信者は当該暗号鍵で平文を暗号化し、受信者は当該暗号鍵で暗号文を平文に復号化する。この場合、通信に先立って送信者と受信者間で同一の暗号鍵を第 3 者に知れること無く、安全に保有することが課題となる。従って、第 1 の方法では、身近な人相互間の通信、相手が判っている人との間での通信に適している。他方、公開鍵暗号

を使用する場合には、予め、暗号通信の利用者ごとに暗号鍵（公開鍵）と復号鍵（秘密鍵）を生成しておき、送信者は受信者の暗号鍵で平文を暗号化し、受信者は自分の復号鍵で暗号文を平文に復号化する。したがって、暗号鍵は暗号通信の不特定多数の利用者に開示され、復号鍵は、特定の 1 人の利用者（メッセージ受信者）のみに知らせることが必要であるが、秘密鍵暗号の前述の課題である同一の暗号鍵を送受信者間で事前に保有する必要はない。従って、第 2 の方法では、知らない相手方との間の通信、電子取引による通信等に適している。

【0003】 ここで、暗号鍵と復号鍵は数学的関数関係を有し、暗号鍵から復号鍵を特定することが計算量的に困難であることが前提となる。例えば、代表的な RSA 暗号においては、50桁以上の素数  $p$ 、 $q$  を選択し、 $n = p \times q$  を求め、復号鍵  $e$  を  $(p-1) \times (q-1)$  と互いに素な整数に設定する。そして、 $d$  を  $e \times d \equiv 1 \pmod{(p-1) \times (q-1)}$  として求め、 $n$  と  $d$  を暗号鍵とする。これにより、復号鍵  $e$  を特定することは、 $n$  から  $p$  と  $q$  を算出することに帰着されるため、50桁以上の素数の素因数分解と同値の計算量的困難性を得る。また、秘密鍵暗号は、コンピュータシステム内に記録された情報に対して、ビット単位の変換処理を特定の量で一括して行い、公開鍵暗号は、コンピュータシステムに記録された情報を数値量とみなして、数学的関数変換を行うため、秘密鍵暗号は、公開鍵暗号に比べて、極めて高速に動作し、消費するコンピュータ資源（メモリ、CPU）は少量ですむ。

【0004】 さらに、秘密鍵暗号、公開鍵暗号とも暗号文の解読の困難性は、暗号鍵の長さに依存する。例えば、秘密鍵暗号の代表的な DES 暗号では、暗号鍵のビットパターンを元に、平文のビットパターンを攪拌し、排他的論理和を取り暗号文を作成する。RSA 暗号では、前述のように選択する素数  $p$  と  $q$  の桁数が多いほど、すなわち公開鍵  $n$ 、 $d$  の桁数が多いほど、秘密鍵の算出が困難になる。そこで、秘密鍵暗号や公開鍵暗号を用いた暗号メッセージ通信では、暗号鍵の長さが長いほど、指数関数的に解読が困難になってくるが、他方暗号化、復号化に必要なコンピュータ資源（CPU、メモリ）と処理時間が指数関数的に多くなる。ところで、従来、取引毎に使用する暗号化方法を変化させ、また暗号化キーデータを不規則に変動させることにより、第 3 者による電文の暗号化データの解読を困難にすることを目的とした電文暗号化方式が提案されている（例えば、特開平 10-105624 号公報参照）。この方法では、利用者が電文の暗号化方法として、例えば銀行と顧客間で残高照会内容を送受信する場合には、暗号化パターン 1 を選択し、磁気カード上の口座番号とパターン 1 の暗号化キーデータの排他的論理和をとり、暗号化口座番号を作成している。しかしながら、上記公報に記載の暗号化方法では、何の根拠もなく、種々のパターンから 1 つを自由に選択

## 3

するものであって、その通信に真に必要な強度の暗号文が得られるかは不明であり、また暗号化に伴う費用も低減できるか否かは不明である。

## 【0005】

【発明が解決しようとする課題】 上述のように、ネットワークコンピューティング環境で、暗号メッセージ通信を行う場合、暗号アルゴリズムや暗号鍵長の選択は、利用者の利便性やコンピュータ経費に大きく影響するため、必要な秘匿性の程度や使い勝手、費用を考慮して選択する必要がある。すなわち、暗号メッセージに必要な解読の困難性の程度は、使用するネットワークの特性やメッセージの内容に依存する場合が多い。例えば、インターネットや無線を使用したメッセージ通信では、通信経路上の暗号メッセージが不特定多数の人にアクセス可能になるため、一般に必要な解読の困難性が高い。他方、専用通信回線を使用したメッセージ通信では、通信経路上の暗号メッセージにアクセス可能な人が特定される為、必要な解読の困難性は相対的に低い。さらに、利用者の立場では、通信メッセージの重要度に応じて必要な解読の困難性が変化することは、言うまでもない。

【0006】 また、前述のように、秘密鍵暗号は公開鍵暗号に比べて高速であり、所要コンピュータ資源も少量であるが、送受信者間で暗号鍵を安全に共有する困難さがあるため、一般に特定グループの人が使用するネットワークの場合（例えば、企業内ネットワーク）には適するが、インターネットなどの不特定の人が使用するネットワークには、公開鍵暗号が適している。しかし、近年のように、ネットワークコンピューティング環境が普及している状況下では、コンピュータシステムからのアクセス可能なネットワークが増加し、メッセージ送信先も多岐に渡っているため、利用者が上記のような暗号アルゴリズムや暗号鍵長を考慮し、多数の種類の中から1つを選択して、それを用いて暗号メッセージ通信を行うことは困難になってきている。

【0007】 そこで、本発明の目的は、従来の暗号メッセージ通信における上述のような問題点を解消し、コンピュータネットワーク上で、暗号メッセージ通信を行う場合に、メッセージの暗号化処理に先立って、使用するネットワークの状況や通信メッセージの内容によって、必要な強度の暗号文が得られ、かつ暗号化に伴う費用を低減できるような暗号通信方法とそのプログラムを記録した記録媒体を提供することにある。

## 【0008】

【課題を解決するための手段】 上記目的を達成するため、本発明の暗号通信方法では、利用者が暗号化処理を行う度毎に、送信先と通信メッセージの秘匿の必要性を、利用者に比較的簡明な情報で指定することにより、使用するネットワークの種類を判別し、暗号アルゴリズムと暗号鍵を選択できるようにして、ネットワークの種類や通信メッセージの内容に適した強度の暗号化方法を

## 4

与える。そのために、受信者名を入力することにより、IP (Internet Protocol) アドレスに変換するようにマッピングしておき、変換されたIPアドレスから使用するネットワークの状況を判別し、またメッセージの重要度を入力することにより、必要な強度の暗号文が得られるように、自動的に最適の暗号アルゴリズムと暗号鍵が選択されるようなテーブルを作成しておく。次に、選択された暗号化アルゴリズムと暗号鍵を用いてメッセージを暗号化し、暗号文の送信および受信を行う。これにより、利用者は容易に暗号通信の安全性を確保しながら、最適な暗号アルゴリズムと必要な長さの暗号鍵を選択することができるので、送信者の負担の軽減とコンピュータ資源の節約を図ることができる。

## 【0009】

【発明の実施の形態】 以下、本発明の実施例を、図面により詳細に説明する。図1は、本発明が適用される通信システムの全体概要図である。図1において、101は送信者用コンピュータ、102は狭域ネットワークであるLAN (Local Area Network)、103はLAN102を介して送信者用コンピュータ101からメッセージを受信する受信者A用コンピュータ、104は遠隔地へのメッセージ送信を行い、特定のコンピュータのみが使用可能な専用回線、105は、専用回線104を介してコンピュータ101からメッセージを受信する受信者B用コンピュータ、106は遠隔地へのメッセージ送信を行い、不特定のコンピュータから使用可能な公衆回線、107は公衆回線106を介してコンピュータ101からメッセージを受信する受信者C用コンピュータ、108は電波によりメッセージ送信を行う無線設備、109は無線設備108を介してコンピュータ101からメッセージを受信する受信者D用コンピュータ、110は常時不特定のコンピュータが使用し、経路が不特定のインターネット、111は、インターネット110を介して、コンピュータ101からメッセージを受信する受信者E用コンピュータ、112はLAN102から専用回線104、インターネット110、公衆回線106および無線設備108へのルートを選択して送信するルータ、113、114、115も受信者B、C、D用コンピュータ105、107、109にそれぞれルートを選択して送信するルータである。

【0010】 図2は、本発明の一実施例を示す通信メッセージの重要度に応じた内容例のテーブルの図である。図2において、201は通信メッセージの暗号文に対して必要となる解読の困難性を3段階（大、中、小）に区分した項目、202は項目201の各段階に該当するメッセージの例である。このテーブルは、送信者用コンピュータ101は勿論のこと、受信者B、C、D、E用コンピュータ105、107、109、111の各メモリに格納されている。受信者用コンピュータも、次回には送信用コンピュータになる可能性を有している。これ例では、

電子決済用のクレジットカード番号や、個人のプライバシー情報を含んだメッセージに対しては解読の困難性が大のものが必要であり、社内の売上げデータを記述したメッセージに対しては、解読の困難性が中程度のものが必要であり、会議案内のようなメッセージは解読の困難性が小のものでよいことが判別される。

【0011】図3は、図1における送信者用コンピュータ内の処理装置のブロック図である。送信者用コンピュータ101で実行される処理装置は、図3に示すような構成となっている。図3において、301は送信者が受信者名（受信者ID）を入力する処理部、302は送信者が通信メッセージに対して必要となる解読の困難性の段階を入力する処理部、303は受信者入力部301と重要度入力部302から入力されたデータをもとに使用する暗号鍵を選択する処理部、304は受信者に対応して、すなわち使用するネットワークの種類と必要な解読の困難性の段階に対応して、選択すべき暗号鍵を登録した暗号鍵登録テーブル、305は鍵長選択部303で選択した暗号鍵にもとずき通信メッセージを暗号化する処理部、306は暗号化処理部305で暗号化した通信メッセージを送信する処理部である。受信者入力部301の入力と通信メッセージの重要度入力部302の入力とを同時に行うか、あるいはシリアルに行うかは任意に決められるが、ここでは、同一画面でほぼ同時に入力された両方の入力データを、入力部301および302にそれぞれ入力して処理する。

【0012】受信者入力部301では、受信者IDが入力されることにより、IP（Internet Protocol）アドレスに変換するようにマッピングされたデータベースが配置されており、変換されたIPアドレスから使用するネットワークの状況を判別して、受信者がLAN102に接続されているか、インターネット110に接続されているか、専用回線104に接続されているか、公衆回線106に接続されているか、あるいは無線回線108に接続されているかを判別し、判別した情報を鍵長選択部303に送る。例えば、IPアドレスの先頭部分の何ビットを判別範囲にしておき、その部分が異なればインターネット、あるいは遠距離回線であると判別する。先頭部分が送信者のIPアドレスと同じであれば、LANであると判別する。一方、メッセージ重要度入力部302では、クレジットカード、プライバシー情報、社内の売上げデータ、社内の会議録、会議案内等の内容が入力されることにより、図2に示すテーブルを検索して必要な解読の困難性の段階を自動的に得る。得られた必要性の段階は、鍵長選択部303に送られる。

【0013】図4は、図3で示した処理ブロック図における暗号鍵登録テーブルの概念図である。図4において、401は使用するネットワーク種別を示す項目、402は通信メッセージに必要な暗号文の解読困難性

の程度を示す項目、403はネットワーク種別401、メッセージ重要度402の項目に対応して使用する暗号アルゴリズムの項目、404は401、402、403の項目に対応した暗号鍵長（ビット数）、405は使用する暗号鍵である。なお、暗号アルゴリズム403において、Desは暗号鍵

図4に示すように、自動的に最適の暗号アルゴリズムと暗号鍵が選択されるようなテーブルを作成しておくことにより、鍵長選択部303は入力されたネットワークの種別とメッセージの重要度に基づいて、このテーブルから暗号化アルゴリズム403と暗号鍵405とを自動的に選択する。そして、これらを暗号処理部305に送る。暗号処理部305では、送られた暗号化アルゴリズム403と暗号鍵405を用いてメッセージを暗号化し、メッセージ送信部306に送る。メッセージ送信部306では、送られた暗号文にヘッダ等の制御文を付加し、各回線に適合した制御を行うことにより暗号メッセージを送信する。

【0014】図5は、本発明の一実施例を示す暗号通信方法の動作フローチャートである。図5において、ステップ501は暗号通信メッセージの受信者名を送信者が入力する処理、ステップ502はステップ501で入力した暗号メッセージの受信者名に基づき、使用されるネットワークの種別を算出する処理、ステップ503は通信メッセージの内容に基づき、送信者が秘匿の必要性の段階を入力する処理、ステップ504はステップ502で求めたネットワークの種別とステップ503で入力された通信メッセージの必要な秘匿性の程度をキーとして、暗号鍵登録テーブルの中から、使用すべき暗号アルゴリズムと暗号鍵を検索する処理、ステップ505は検索処理ステップ504の結果、一致する暗号アルゴリズムと暗号鍵が暗号鍵登録テーブル中に存在したか否かを判定する判定処理、ステップ506は通信メッセージの平文を暗号化する処理、ステップ507は暗号文を送信する処理、ステップ508は平文を送信する処理である。

【0015】次に、図5を用いて、本発明の動作を説明する。まず、送信者用コンピュータ上から送信者が受信者IDを入力する（ステップ501）。次に、受信者IDをIPアドレスなどに変換することにより、使用するネットワークの経路、種別を算出する（ステップ502）。次に、送信者用コンピュータ上から、送信者は、メッセージの重要度に応じて必要な秘匿性の程度を‘大’、‘中’、‘小’の三段階から選択して入力する（ステップ503）。これにより、図4の暗号鍵登録テーブルを検索する（ステップ504）。暗号鍵登録テーブルの検索結果を判定し（ステップ505）、ステップ502で算出したネットワーク種別、ステップ503で入力した必要な秘匿性の程度に該当する暗号アルゴリズムと暗号鍵が登録されていない場合には、通信メッセージを平文で送

信する(ステップ508)。他方、暗号鍵登録テーブルの検索結果判定により(ステップ505)、該当する暗号アルゴリズムと暗号鍵が登録されている場合は、当該アルゴリズムと暗号鍵でメッセージを暗号化し(ステップ506)、当該暗号文を送信する(ステップ507)。

【0016】このように、本実施例においては、利用者は受信者ID情報と通信メッセージの重要性を指定すれば、暗号メッセージに対して、必要な秘匿性を確保しつつ、コンピュータ消費資源が少なく、使い勝手の良い暗号を利用することができる。また、前述のように、本発明に係わる暗号化手順を選択する処理ステップをコンピュータプログラムで実現する場合、このプログラムをCD-ROM等の記録媒体に記録した形態で、商品として流通させることが可能である。また、この記録媒体を任意の場所に設置されたパーソナルコンピュータに挿入して、プログラムをインストールすることにより、あるいは通信回線を介して他のコンピュータから転送してインストールすることにより、任意の時刻に本発明を実現して、必要な暗号鍵とアルゴリズムを自動選択して暗号メッセージ送信することができる。

#### 【0017】

【発明の効果】以上説明したように、本発明によれば、ネットワークコンピューティング環境が下において、暗号通信の利用者は、容易に暗号通信の安全性を確保しつつ、最適な暗号アルゴリズムを選択可能になるため、送信者の負担軽減やコンピュータ資源の節減が図れる。さらに、通信メッセージの重要度に応じて暗号アルゴリ

ズムと必要な長さの暗号鍵が選択できるため、全体的に暗号通信の安全性が高まるという効果がある。

#### 【図面の簡単な説明】

【図1】本発明が適用される通信システムの全体概要図である。

【図2】本発明の一実施例を示す通信メッセージの重要度に応じた内容例のテーブル図である。

【図3】図1における送信者用コンピュータに内蔵された処理ブロック図である。

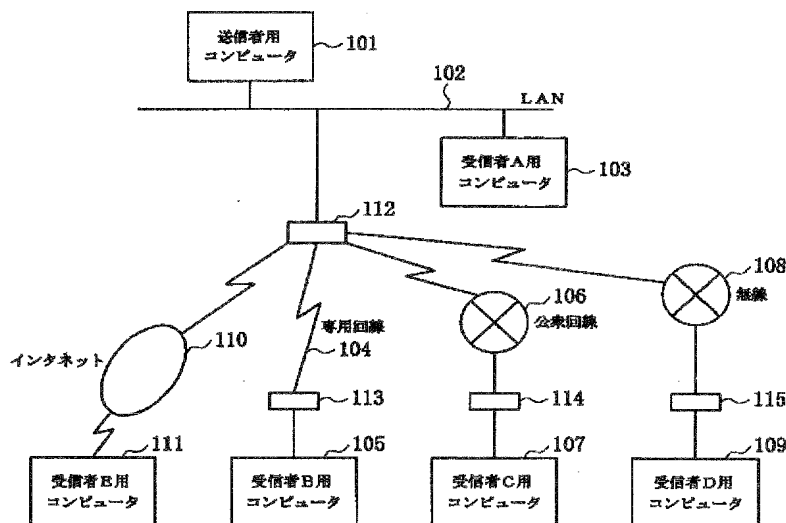
10 【図4】図3における暗号鍵登録テーブルのフォーマット図である。

【図5】本発明の一実施例を示す暗号通信方法の動作フローチャートである。

#### 【符号の説明】

101…送信者用コンピュータ、102…LAN (Local Area Network)、103…受信者A用コンピュータ、104…専用回線、105…受信者B用コンピュータ、106…公衆回線、107…受信者C用コンピュータ、108…無線設備、109…受信者D用コンピュータ、110…インターネット、111…受信者E用コンピュータ、112…ルータ、201…必要な解読の困難性の段階の欄、202…段階に対するメッセージ、301…受信者ID入力部、302…メッセージ重要度入力部、303…鍵長選択部、304…暗号鍵登録テーブル、305…暗号処理部、306…メッセージ送信部、401…ネットワーク種別、402…メッセージ重要度、403…暗号アルゴリズム、404…鍵長、405…暗号鍵。

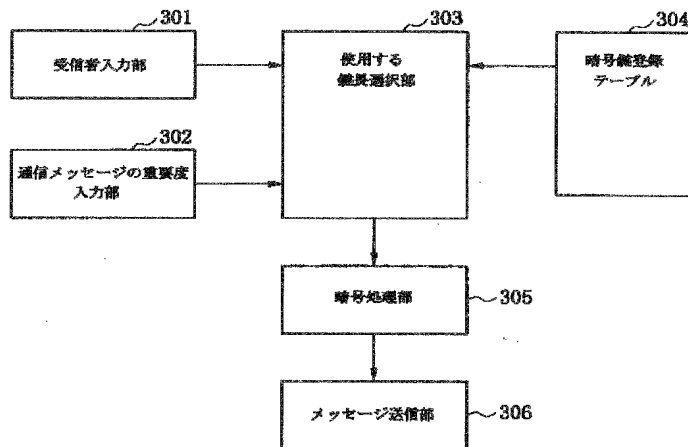
【図1】



【図2】

201 必要な 解読の困難性	202 メッセージの例
大	・電子決済用のクレジットカード番号 ・個人のプライバシー情報
中	・社内の売上げデータ
小	・会費案内

【図 3】



【図 4】

401 ネットワーク 種別	402 メッセージ 重要度	403 暗号アルゴリズム	404 鍵長 (ビット)	405 暗号鍵
LAN	大	Des	40	0110...10
専用	大	Des	56	1100100...10
公衆	大	RSA	128	1111001010...0101
専用	中	RSA	64	011011...1001
インターネット	大	RSA	256	11001.....0110001
インターネット	中	RSA	128	10010100...1001
無線	大	RSA	256	00101.....10011110
インターネット	中	RSA	128	01100100...1010

【図5】

